843.42990X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	MASUOKA, et al.
Serial No.:	Not yet assigned
Filed:	July 30, 2003
Title:	NETWORK MONITORING METHOD FOR INFORMATION SYSTEM, OPERATIONAL RISK EVALUATION METHOD, SERVICE BUSINESS PERFORMING METHOD, AND INSURANCE BUSINESS MANAGING METHOD
Group:	Not yet assigned

LETTER CLAIMING RIGHT OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

July 30, 2003

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2003-048456, filed February 26, 2003.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Ronald J. Shore

~~James N. Dresser~~
~~Registration No. 22,973~~
Ronald J. Shore
Reg. No. 28,577

JND/alb
Attachment
(703) 312-6600

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００３年　２月２６日

出願番号
Application Number:　特願２００３－０４８４５６

[ST.10/C]:　[ＪＰ２００３－０４８４５６]

出願人
Applicant(s):　株式会社日立製作所

２００３年　５月２３日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０３７８７６

【書類名】　特許願
【整理番号】　H02013741
【提出日】　平成15年 2月26日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
　　G06F 19/00
【発明者】
　【住所又は居所】　東京都国分寺市東恋ヶ窪一丁目２８０番地　株式会社日立製作所　中央研究所内
　【氏名】　増岡　義政
【発明者】
　【住所又は居所】　東京都国分寺市東恋ヶ窪一丁目２８０番地　株式会社日立製作所　中央研究所内
　【氏名】　直野　健
【発明者】
　【住所又は居所】　東京都国分寺市東恋ヶ窪一丁目２８０番地　株式会社日立製作所　中央研究所内
　【氏名】　亀山　伸
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社日立製作所
【代理人】
　【識別番号】　100080001
　【弁理士】
　【氏名又は名称】　筒井　大和
　【電話番号】　03-3366-0787
【手数料の表示】
　【予納台帳番号】　006909
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報システムのネットワーク監視方法及びオペレーショナルリスク計量方法

【特許請求の範囲】

【請求項１】　ネットワークに接続されアプリケーションを実行する１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算機内の操作履歴を収集するステップと、

前記ネットワークに接続され前記ネットワークを監視する１つ以上の第２の計算機において、前記エージェントが実行されていない前記第１の計算機の存在を監視して記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのネットワーク監視方法。

【請求項２】　ネットワークに接続されアプリケーションを実行する１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算機内の操作履歴を収集するステップと、

前記ネットワークに接続され前記ネットワークを監視する１つ以上の第２の計算機において、前記ネットワークを流れるパケットを傍受するステップと、

前記第２の計算機において、前記傍受したパケットから送信元及び／又は送信先のアドレスを取り出すステップと、

前記第２の計算機において、前記アドレスに対応する前記第１の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第２の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第１の計算機の前記アドレスを記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのネットワーク監視方法。

【請求項３】　ネットワークに接続されアプリケーションを実行する１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算

機内の操作履歴を収集するステップと、

前記ネットワークに接続され前記ネットワークを監視する１つ以上の第２の計算機において、前記ネットワークを構成するネットワーク機器と通信して、前記ネットワーク機器に接続された前記第１の計算機のアドレスリストを取得するステップと、

前記第２の計算機において、前記取得したアドレスリスト内のアドレスに対応する前記第１の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第２の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第１の計算機の前記アドレスを記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのネットワーク監視方法。

【請求項４】　ネットワークに接続されアプリケーションを実行する１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され前記ネットワークを監視する１つ以上の第２の計算機において、前記エージェントが実行されていない前記第１の計算機の存在を監視して記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのオペレーショナルリスク計量方法。

【請求項５】　ネットワークに接続されアプリケーションを実行する１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され前記ネットワークを監視する１つ以上の第２の計算機において、前記ネットワークを流れるパケットを傍受するステップと、

前記第２の計算機において、前記傍受したパケットから送信元及び／又は送信先のアドレスを取り出すステップと、

前記第２の計算機において、前記アドレスに対応する前記第１の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第２の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第１の計算機の前記アドレスを記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのオペレーショナルリスク計量方法。

【請求項６】　ネットワークに接続されアプリケーションを実行する１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され前記ネットワークを監視する１つ以上の第２の計算機において、前記ネットワークを構成するネットワーク機器と通信して、前記ネットワーク機器に接続された前記第１の計算機のアドレスリストを取得するステップと、

前記第２の計算機において、前記取得したアドレスリスト内のアドレスに対応する前記第１の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第２の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第１の計算機の前記アドレスを記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのオペレーショナルリスク計量方法。

【請求項７】　ネットワークに接続されアプリケーションを実行する顧客企

業所有の１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算機内の操作履歴を収集するステップと、

前記ネットワークに接続されサービス事業者の管理の下に設置された１つ以上の第２の計算機において、前記エージェントが実行されていない前記第１の計算機の存在を監視して記録に残すステップと、

前記サービス事業者において、前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする顧客企業のオペレーショナルリスクの正確性を公証するサービス事業の実施方法。

【請求項８】　ネットワークに接続されアプリケーションを実行する顧客企業所有の１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算機内の操作履歴を収集するステップと、

前記ネットワークに接続されサービス事業者の管理の下に設置された１つ以上の第２の計算機において、前記ネットワークを流れるパケットを傍受するステップと、

前記第２の計算機において、前記傍受したパケットから送信元及び／又は送信先のアドレスを取り出すステップと、

前記第２の計算機において、前記アドレスに対応する前記第１の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第２の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第１の計算機の前記アドレスを記録に残すステップと、

前記サービス事業者において、前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする顧客企業のオペレーショナルリスクの正確性を公証するサービス事業の実施方法。

【請求項９】　ネットワークに接続されアプリケーションを実行する顧客企業所有の１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され保険業者の管理の下に設置された１つ以上の第２の計算機において、前記エージェントが実行されていない前記第１の計算機の存在を監視して記録に残すステップと、

前記保険業者において、前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップと、

を有することを特徴とする顧客企業のオペレーショナルリスクに該当する事象により発生した損失を補填する保険業の運営方法。

【請求項１０】　ネットワークに接続されアプリケーションを実行する顧客企業所有の１つ以上の第１の計算機において、１つ以上のエージェントを実行して前記第１の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され保険業者の管理の下に設置された１つ以上の第２の計算機において、前記ネットワークを流れるパケットを傍受するステップと、

前記第２の計算機において、前記傍受したパケットから送信元及び／又は送信先のアドレスを取り出すステップと、

前記第２の計算機において、前記アドレスに対応する前記第１の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第２の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第１の計算機の前記アドレスを記録に残すステップと、

前記保険業者において、前記記録を検査し、情報システムを構成する前記第１の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップと、

を有することを特徴とする顧客企業のオペレーショナルリスクに該当する事象により発生した損失を補填する保険業の運営方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク監視方法及びオペレーショナルリスク計量方法などに関し、特にネットワークを利用した複数の計算機を含む情報処理システムのオペレーショナルリスク計量技術に適用して有効な技術に関する。

【０００２】

【従来の技術】

近年、非特許文献１に記載されているように、企業（非営利団体や一般の組織も含む。以下、これらの総称として「企業」という）は、その健全性を維持するためのリスク管理の一方法として、その内部の情報システムの操作ミスや情報システム内で発生した障害などによって受ける損失額をリスクとして計量しようとしている。この種のリスクは、「オペレーショナルリスク（Ｏｐｅｒａｔｉｏｎａｌ　Ｒｉｓｋ）」と呼ばれており、特に金融機関ではその重要性が高い。どのような事象をオペレーショナルリスクとして判断するか、オペレーショナルリスクに該当する各事象をどのように分類するか、については、前記非特許文献１に、現状の定義が記載されている。

【０００３】

また、非特許文献２によれば、オペレーショナルリスクは、例えば、次の方法によって計量できる。まず、過去の企業内部及び外部のデータを収集・蓄積し、損失の発生した事象を示す元となるデータ（以下、「損失イベント（ｏｐｅｒａｔｉｏｎａｌ　ｌｏｓｓ　ｅｖｅｎｔ）」という）を集める。次に、収集した損失イベントに対し、一定の計算を行うことにより、オペレーショナルリスクを計量する。

【０００４】

現在の企業では、ほとんどすべての業務が何らかの形で情報システムを利用して遂行されている。この情報システムは、通常、ネットワークに接続された複数の計算機（端末やサーバなど）で業務アプリケーションを実行させている。そのため、前記損失イベントの収集においては、情報システムの運用管理機能において、エラーログなどの操作履歴情報を取得することが重要である。運用管理機能については、特許文献１や特許文献２などに記載されている。これらの運用管理

機能では、ネットワーク内を流れる情報を傍受することにより、ネットワークに接続された計算機等の構成図を作成することができる。

【０００５】

【特許文献１】

米国特許第５９４８０５５号明細書

【０００６】

【特許文献２】

米国特許第５７８７２５２号明細書

【０００７】

【非特許文献１】

バーゼル・コミッティ・オン・バンキング・スーパービジョン（Ｂａｓｅｌ Ｃｏｍｍｉｔｅｅ ｏｎ Ｂａｎｋｉｎｇ Ｓｕｐｅｒｖｉｓｉｏｎ）編，「ワーキング・ペーパ・オン・ザ・レギュラトリ・トリートメント・オブ・オペレーショナル・リスク（Ｗｏｒｋｉｎｇ Ｐａｐｅｒ ｏｎ ｔｈｅ Ｒｅｇｕｌａｔｏｒｙ Ｔｒｅａｔｍｅｎｔ ｏｆ Ｏｐｅｒａｔｉｏｎａｌ Ｒｉｓｋ）」，国際決済銀行，２００１年９月

【０００８】

【非特許文献２】

三菱信託銀行オペレーショナル・リスク研究会編，「オペレーショナル・リスクのすべて」，東洋経済新報社，２００２年３月，ｐ．１０７－１５７

【０００９】

【発明が解決しようとする課題】

ところで、前記のようなオペレーショナルリスク計量の技術について、本発明者が検討した結果、以下のようなことが明らかとなった。

【００１０】

オペレーショナルリスクを計量するためには、企業内部の損失イベントの収集が不可欠である。しかしながら、前記の従来の技術では、オペレーショナルリス

クをリスク管理に活用するには、次の点で問題がある。

【００１１】

すなわち、その企業内で業務に用いられているすべての計算機から、損失イベントを収集したか否か、確認する方法がない。そのため、オペレーショナルリスクを計量する際に収集した損失イベントが、その企業内で発生した損失イベントのすべてか否か、又は、オペレーショナルリスク計量のために許容される誤算の範囲で十分か否かが確認できない。

【００１２】

例えば、ある計算機の操作ミスによって，その企業に損失が発生したとする。もし、この計算機が損失イベントの情報収集の対象になっていないとき、計量されたオペレーショナルリスクは、不当に低く算出されてしまうことになる。これでは、企業の経営の一環としてオペレーショナルリスクの管理を適切に行うことも、オペレーショナルリスクの管理を適切に行っていることを外部に示すこともできない。

【００１３】

そこで、本発明の第１の目的は、オペレーショナルリスク計量のために、企業内で業務に用いられているすべての計算機から損失イベントを収集したか否かを確認することができるネットワーク監視方法を提供することである。

【００１４】

本発明の第２の目的は、前記ネットワーク監視方法を用いた、オペレーショナルリスク計量方法を提供することである。

【００１５】

本発明の第３の目的は、前記ネットワーク監視方法を用いた、オペレーショナルリスク計量のためのサービス方法を提供することである。

【００１６】

本発明の前記並びにその他の目的と新規な特徴は、本明細書の記述及び添付図面から明らかになるであろう。

【００１７】

【課題を解決するための手段】

本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、次のとおりである。

【００１８】

すなわち、本発明によるネットワーク監視方法及びオペレーショナルリスク計量方法においては、企業のネットワークに接続されアプリケーションを実行する１つ以上の第１の計算機（業務実行計算機）に、その計算機内で発生した損失イベントを収集するためのエージェントを１つ以上設ける。また、その企業のネットワークに接続されネットワークを監視する第２の計算機（ネットワーク監視サーバ機）を１つ以上設ける。当該第２の計算機は、当該ネットワークを監視し、第１の計算機の中に、前記エージェントが設けられていない計算機があれば、その旨を記録に追加する。

【００１９】

前記第２の計算機が前記ネットワークを監視する方法としては、当該ネットワークを流れるパケットを傍受し、当該パケットから送信元及び／又は送信先のアドレスを取り出し、取り出したアドレスに対応する計算機の前記エージェントに対してメッセージを送信し、当該送信メッセージに対する応答を確認する方法がある。

【００２０】

また、前記第２の計算機が前記ネットワークを監視する他の方法としては、前記ネットワークがネットワーク機器（ルータなど）に接続されていて、当該ネットワーク機器がパケットを中継した計算機のアドレスリストを保持している場合は、前記第２の計算機が前記ネットワーク機器と通信して当該アドレスリストを取得し、当該アドレスリスト内のアドレスに対応する計算機の前記エージェントに対してメッセージを送信し、当該送信メッセージに対する応答を確認する方法もある。この場合は、パケットを傍受する必要がないため、工数を軽減することができる。

【００２１】

また、オペレーショナルリスク計量方法としては、前記第１の計算機内で発生した損失イベントを収集するためのエージェントを実行し、前記第１の計算機内

の操作履歴を収集し、当該操作履歴から損失の発生した事象を抽出し、当該事象における損失額を決定し、オペレーショナルリスクを計量する方法がある。

【００２２】

したがって、前記ネットワーク監視方法及び前記オペレーショナルリスク計量方法によれば、前記エージェントによって収集された損失イベントから、オペレーショナルリスクを計量することができるだけでなく、前記第２の計算機の前記記録を検査することにより、企業内で業務に用いられる計算機すべてにおいて損失イベントを収集したことを確認することができる。

【００２３】

すなわち、もし、前記記録に何も記載がなければ、企業内で業務に用いられるすべての計算機に前記エージェントが設けられており、すべての計算機から損失イベントが収集されたことを確認することができる。あるいはもし、前記記録に記載があれば、当該記録に記載された、前記エージェントが設けられていない計算機については、別途、手作業や聞き取りによる調査を行うことにより、企業内のすべての前記計算機から損失イベントを収集することができる。

【００２４】

また、情報システムを保有する企業に対して、別のサービス事業者が、前記第２の計算機を設置し、前記企業の情報システムのネットワークに接続することにより、当該企業のオペレーショナルリスクの正確性を公証するサービスを提供することができる。

【００２５】

また、保険業者等が前記オペレーショナルリスク計量方法を顧客企業の情報システムに適用することにより、前記顧客企業のオペレーショナルリスクに該当する事象により発生した損失を正確に計量することが可能となり、当該損失を補填したり、当該計量結果に基づいて保険料を決定したりする保険業を運営することができる。

【００２６】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。なお、実施の形

態を説明するための全図において、同一部材には同一の符号を付し、その繰り返しの説明は省略する。

【００２７】

（ハードウェア構成）

図１は、本発明の一実施の形態における情報システムのハードウェア構成を示す図である。本実施の形態における企業の情報システム１００は、ネットワーク１０１を有している。ネットワーク１０１は、企業内の各計算機を、リンク１０２によって接続している。リンク１０２は、有線でも無線でもよい。また、図１に図示していないが、ネットワーク１０１は、企業外の計算機と通信するためのリンクを有していてもよい。

【００２８】

情報システム１００は、３種類の計算機を有している。具体的には、業務実行計算機（第１の計算機）１０３ａ，１０３ｂ，…、運用管理サーバ機１０４、ネットワーク監視サーバ機（第２の計算機）１０５である。

【００２９】

業務実行計算機１０３ａ，１０３ｂ，…は、具体的には端末、パーソナルコンピュータ、サーバ計算機、メインフレーム、ネットワーク機器などであり、ネットワーク１０１に接続され、業務実行計算機１０３ａ，１０３ｂ，…の間で必要に応じて通信しながら、情報システム１００を有する企業の業務を分担して実行する。図１に図示していないが、業務実行計算機１０３ａ，１０３ｂ，…は、１つ以上のプロセッサ，記憶装置，ネットワークインタフェースを有している。また、業務実行計算機１０３ａ，１０３ｂ，…のそれぞれは、その利用方法によって、磁気ディスクや外部記憶装置を備えている場合がある。磁気ディスクや外部記憶装置も、図１には図示していない。

【００３０】

運用管理サーバ機１０４は、図１では１つしか図示していないが、複数設けられていてもよい。運用管理サーバ機１０４は、ネットワーク１０１に接続されている。運用管理サーバ機１０４は、損失イベントを収集し、オペレーショナルリスクを計算するための計算機である。図１に図示していないが、１つ以上のプロ

セッサ，記憶装置，ネットワークインタフェースを有している。

【００３１】

ネットワーク監視サーバ機１０５は、図１では１つしか図示していないが、複数設けられていてもよい。ネットワーク監視サーバ機１０５は、ネットワーク１０１に接続されている。ネットワーク監視サーバ機１０５は、ネットワーク１０１を監視し、後述するエージェント１１０が設けられていない計算機が情報システム１００に接続されていることを監視、検出するための計算機である。図１に図示していないが、１つ以上のプロセッサ，記憶装置，ネットワークインタフェースを有している。

【００３２】

なお、本実施の形態では、業務実行計算機１０３ａ，１０３ｂ，…、運用管理サーバ機１０４、ネットワーク監視サーバ機１０５をそれぞれ別の筐体の計算機として扱うが、実際にはどれか２つ、または３種類すべてが、同じ筐体に格納されていてもよい。

【００３３】

（ソフトウェア構成）

図１を用いて、本実施の形態のソフトウェア構成、すなわちプログラムとデータの構成を説明する。

【００３４】

業務実行計算機１０３ａ，１０３ｂ，…上では、エージェント１１０が実行される。エージェント１１０は、データ収集部１１１と確認応答部１１２を含むプログラムで、業務実行計算機１０３ａ，１０３ｂ，…のプロセッサにより実行される。

【００３５】

データ収集部１１１は、業務実行計算機１０３ａ，１０３ｂ，…内の履歴情報１１５ａ，１１５ｂ，…の内容を一定間隔で読み込み、ネットワーク１０１を通して運用管理サーバ機１０４のデータ集計部１３１へ送信する。

【００３６】

確認応答部１１２は、ネットワーク監視サーバ機１０５の検出部１２２から問

合せメッセージが送られてくるのを待ち、当該問い合わせメッセージが送られてきたら、送信元の検出部１２２に応答メッセージを送信する。図４を用いて後述するが、検出部１２２は、当該問合せメッセージを用いることにより、業務実行計算機１０３ａ，１０３ｂ，…上でエージェント１１０が実行されているか否かを確認する。

【００３７】

図１に図示していないが、業務実行計算機１０３ａ，１０３ｂ，…上では、エージェント１１０の他に、企業の業務を行うアプリケーションプログラムも１つ以上実行される。当該アプリケーションのそれぞれは、過去のログや、エラーメッセージや、実行経過のトレース情報や、稼動統計情報を、履歴情報１１５ａ，１１５ｂ，…に出力している。履歴情報１１５ａ，１１５ｂ，…は、磁気ディスク上のファイルや、運用コマンドの出力結果などの形で、エージェント１１０のデータ収集部１１１から、データとして参照可能である。

【００３８】

運用管理サーバ機１０４では、３つのプログラムが実行される。すなわち、データ集計部１３１、計量部１３２、及び結果表示部１３３である。これらのプログラムの動作は、図３を用いて後でより詳細に説明するが、データ集計部１３１は、エージェント１１０のデータ収集部１１１から送信されてきた履歴情報を集計し、計量部１３２はデータ集計部１３１の集計結果からオペレーショナルリスクを計量し、結果表示部１３３は計量したオペレーショナルリスクを表示する。なお、その他のプログラムが、運用管理サーバ機１０４で実行されてもよい。

【００３９】

ネットワーク監視サーバ機１０５では、パケット監視部１２１と、検出部１２２の、２つのプログラムが実行される。パケット監視部１２１は、ネットワーク監視サーバ機１０５が備えるネットワークインタフェースを利用し、ネットワーク１０１を流れるパケットを傍受する。当該パケットの構造及び内容を図２に示す。検出部１２２は、パケット監視部１２１が傍受したパケットを受け取り、そのパケットから送信元のアドレスと送信先のアドレスを取り出して、そのアドレスが割り当てられた業務実行計算機１０３ａ，１０３ｂ，…においてエージェン

ト１１０が実行されているか否か確認する。また、検出部１２２は、当該処理のため、２種類のデータ、すなわちアドレスリスト１２５と監視ログ１２６を保持する。アドレスリスト１２５は、通常主記憶内に格納されるが、磁気ディスク上でもよい。監視ログ１２６は、通常磁気ディスク内に格納される。なお、検出部１２２の動作は、後で図４を用いてより詳しく説明する。

【００４０】

なお，図１には図示していないが、各計算機にはオペレーティング・システムが主記憶にロードされ、当該計算機のプロセッサにより実行される。前記のエージェント１１０などの各プログラムは、当該オペレーティング・システムによって実行を管理されている。また、前記の各プログラムは、必要に応じて、当該オペレーティング・システムに要求を出すことにより、ネットワーク通信、ファイルや磁気ディスク上のデータへのアクセスなどを行うことができる。

【００４１】

なお、本実施の形態において、業務実行計算機１０３ａ，１０３ｂ，…のエージェント１１０、データ収集部１１１、確認応答部１１２、運用管理サーバ機１０４のデータ集計部１３１、計量部１３２、結果表示部１３３、及びネットワーク監視サーバ機１０５のパケット監視部１２１、検出部１２２は、いずれもプログラムとして取り扱ったが、これらと同等の機能を有していれば、プログラム以外のものであってもよい。

【００４２】

（ネットワーク通信）

図１に示すように、ネットワーク１０１は、業務実行計算機１０３ａ，１０３ｂ，…、運用管理サーバ機１０４、及びネットワーク監視サーバ機１０５を相互接続する。

【００４３】

ネットワークへの接続について、より具体的に述べると、前記各計算機は、それぞれネットワークインタフェース（図１では図示していない）を有し、このネットワークインタフェースがリンク１０２を通してネットワーク１０１に接続されている。

【００４４】

それぞれのネットワークインタフェースには、一意なネットワークアドレス（以下「アドレス」と略す）を割り当てる。このアドレスにより、各計算機間の通信は、次のように実現される。すなわち、送信する側が送信先のアドレスと、送りたいデータを格納している主記憶装置上の領域を指定して、自分のネットワークインタフェースに司令を送ることにより、ネットワーク１０１を経由して、パケット２００（図２）が送信される。パケット２００は、前記送信先のアドレスが割り当てられたネットワークインタフェースによって受信され、受信する側で指定した主記憶装置上の領域に書き込まれる。図２に示すように、パケット２００は、送信先アドレス２０１、送信元アドレス２０２、データ２０３を含む。

【００４５】

以上の、「各ネットワークインタフェースに一意のアドレスを割り当てたとき、送信側が送信先のアドレスを指定することによって、送信したいデータが、指定したアドレスが割り当てられたネットワークインタフェースを有する装置に正しく届けられる」という機能を実現する通信方式についてのより具体的な説明は、文献「W. Richard Stevens, “UNIX（登録商標） Network Programming”, Prentice－Hall, p. １７１－１９６」に述べられている。本実施の形態の情報システムにおいては、当該通信方式が確立しているものとし、本明細書では、当該通信方式についてのこれ以上の詳細な説明は省略する。

【００４６】

（オペレーショナルリスク計量方法）

図３に、本実施の形態におけるオペレーショナルリスクの計量方法を示す。本実施の形態では、オペレーショナルリスクの計量は、図１の運用管理サーバ機１０４のデータ集計部１３１、計量部１３２、及び結果表示部１３３によって行われる。

【００４７】

まず、データ集計部１３１は、業務実行計算機１０３ａ，１０３ｂ，…上のエージェント１１０から送信された履歴情報を受信する（ステップＳ３０１）。次

に、データ集計部１３１は、受信した履歴情報の内容を解析して、損失イベントに該当する事象なのか、どのような種類の損失イベントなのかを、判定結果から損失イベントを抽出する（ステップＳ３０２）。より具体的には、前記判定には、例えば履歴情報に含まれるエラーメッセージがあらかじめ登録された文字列パターンと一致するか否かを検査する手法や、履歴情報の内容を適当なディスプレイに表示させて、表示を見た企業の担当者が該当する損失イベントを選択肢から選び、入力するなどの手法を用いる。

【００４８】

次に、データ集計部１３１は、抽出した損失イベントに対し、企業が被った損失の額を決定する（ステップＳ３０３）。より具体的には、例えば抽出した損失イベントのそれぞれにおいて、発生日時、発生場所、損失イベントの種類をディスプレイに表示し、ディスプレイを見た担当者が過去の事故報告書を参照して、当該損失イベントと発生日時と発生場所が一致する報告書を抽出し、当該報告書に記載の損失額を当該損失イベントの損失額として入力するなどの手法を用いる。

【００４９】

次に、データ集計部１３１は、ステップＳ３０３で作成した、抽出した損失イベントと損失額の組合せを、運用管理サーバ機１０４の記憶装置に蓄積する（ステップＳ３０４）。

【００５０】

次に、計量部１３２は、データ集計部１３１が記憶装置に蓄積した、損失イベントと損失額の組合せから、オペレーショナルリスクを計算する（ステップＳ３０５）。より具体的な計算方法としては、例えば、前記非特許文献２に記載された方法を用いればよい。計量部１３２は、計算結果を、結果表示部１３３に渡す。

【００５１】

前記計算結果を渡された結果表示部１３３は、オペレーショナルリスクの計算結果を、ディスプレイ等の出力装置に表示したり、記憶装置中のファイルに格納したり、ネットワーク１０１を通して他の計算機に送信したりして，企業が当該

計算結果をリスク管理に利用できるようにする（ステップＳ３０６）。

【００５２】

（エージェントの設けられていない計算機の検出方法）

図４に、本実施の形態において、エージェントの設けられていない計算機が情報システム１００のネットワーク１０１に接続されていないか否か検出する方法を示す。この処理は、ネットワーク監視サーバ機１０５の検出部１２２において行われる。

【００５３】

まず、検出部１２２は、パケット監視部１２１から渡されたパケット２００（図２）から、送信元アドレスを取り出す（ステップＳ４０１）。次に、アドレスリスト１２５を参照し、取り出した送信元アドレス２０２が、アドレスリスト１２５に登録されているか否かを調べる（ステップＳ４０２）。もし、当該送信元アドレス２０２が、アドレスリスト１２５に登録されていれば、ステップＳ４０９に移行する（ステップＳ４０３）。もし、登録されていなければ、送信元アドレス２０２に該当する計算機上のエージェント１１０を宛先とする問い合わせメッセージを作成し、ネットワーク１０１に送信する（ステップＳ４０４）。

【００５４】

さらに、検出部１２２は、送信した問い合わせメッセージに対する応答がネットワーク監視サーバ機１０５に到来するのを一定時間待つ（ステップＳ４０５）。具体的な待ち時間は、企業において、設定できるようにすれば良い。もし、一定時間内に応答が到着したら（ステップＳ４０６）、アドレスリスト１２５に、ステップＳ４０１で取り出した送信元アドレス２０２を追加する（ステップＳ４０８）。もし、応答が到着しなかったら、監視ログ１２６に、ステップＳ４０１で取り出した送信元アドレス２０２を追加する（ステップＳ４０７）。ステップＳ４０７では、後日の調査のために、監視ログ１２６に、送信元アドレス２０２だけではなく、現在の時刻、パケットの内容なども追加してもよい。また、ステップＳ４０７では、担当者が直ちに調査を始められるように、当該担当者の端末にメッセージを表示したりする処理を実行してもよい。検出部１２２は、ステップＳ４０７、ステップＳ４０８のどちらかを実行後、ステップＳ４０９に移行す

る。

【００５５】

次に，検出部１２２は、ステップＳ４０１からステップＳ４０８までの各ステップを、パケット監視部から渡されたパケット２００（図２）の送信先アドレス２０１についても行う（ステップＳ４０９）。

【００５６】

以上の手順により、ネットワーク１０１に、エージェントの設けられていない計算機が接続されていた場合、当該計算機がネットワーク１０１を通して通信した時点で当該計算機のアドレスを監視ログ１２６に残すことができる。したがって、オペレーショナルリスクの計量時に、監視ログ１２６を検査することにより、企業内で業務に用いているすべての計算機から損失イベントを抽出したか否かを確認することができる。

【００５７】

すなわち、本実施の形態によれば、ネットワーク監視サーバ機１０５の監視ログ１２６に、何も記載がなければ、企業内で業務に用いられる計算機すべてにエージェント１１０が設けられていることとなり、損失イベントがすべての前記計算機から収集されたことを確認することができる。もし、監視ログ１２６に記載があれば、監視ログ１２６に記載された、エージェント１１０が設けられていない計算機については、別途、手作業や聞き取りによる調査を行うことにより、企業内のすべての計算機から損失イベントを収集することが可能である。

【００５８】

（ネットワーク監視方法の変形例）

本実施の形態では、ネットワーク１０１を流れるパケット２００（図２）をネットワーク監視サーバ機１０５のパケット監視部１２１が傍受し、検出部１２２に渡すことによって、エージェントの設けられていない計算機を検出している。以下にその変形例を２つ述べる。

【００５９】

第１の変形例は、情報システムのネットワークが、実際はサブネットワークの組合せから構成されている場合に用いられる。図５は、第１の変形例における情

報システムのハードウェア及びソフトウェアを示す構成図である。図５では、企業の情報システム５００の各計算機を接続しているのは、２つのサブネットワーク５０１Ａ，５０１Ｂと，２つのサブネットワーク間でパケットを中継するルータ５０２などのネットワーク機器である。情報システム５００では、業務実行計算機５０３Ａａ，５０３Ａｂ，…，５０３Ｂａ，５０３Ｂｂ，…は、２つのサブネットワーク５０１Ａ，５０１Ｂに分散して接続されている。より具体的には、業務実行計算機５０３Ａａ，５０３Ａｂ，…は、サブネットワーク５０１Ａに，業務実行計算機５０３Ｂａ，５０３Ｂｂ，…は、サブネットワーク５０１Ｂに接続されている。なお、図５には示されていないが、ネットワーク監視サーバ機５０５Ａ，５０５Ｂには、図１に示す構成と同様に、検出部、アドレスリスト及び監視ログなどが含まれる。また、サブネットワーク５０１Ａ，５０１Ｂには、運用管理サーバ機が接続される。

【００６０】

この場合、ネットワーク監視サーバ機５０５Ａ，５０５Ｂは、それぞれのサブネットワーク５０１Ａ，５０１Ｂに対し、１つ以上接続する構成にすればよい。図５では、ネットワーク監視サーバ機５０５Ａはサブネットワーク５０１Ａに接続し、パケット監視部１２１がサブネットワーク５０１Ａのパケットを傍受するようにする。また、ネットワーク監視サーバ機５０５Ｂはサブネットワーク５０１Ｂに接続し、パケット監視部１２１がサブネットワーク５０１Ｂのパケットを傍受するようにする。

【００６１】

これにより、ネットワーク監視サーバ機が一つのサブネットワークだけに接続されている結果、他のサブネットワーク内を流れるパケットを取得できなくなるおそれを防ぐことができる。なお、ここでは、図５を用いて、サブネットワークが２つの場合について説明したが、サブネットワークが３つ以上の場合も同様である。

【００６２】

第２の変形例は、情報システム１００のネットワーク１０１が、１つ以上のスイッチ又はルータなどのネットワーク機器に接続されていて、当該ネットワーク

機器が、過去に自分がパケットを中継した計算機のアドレスのリストを保持していて、当該リストを運用コマンド等によって一覧表示する機能を持っている場合である。

【００６３】

当該ネットワーク機器がこのような機能を持っている場合は、ネットワーク監視サーバ機１０５は、パケット監視部１２１に代えて、一定間隔で当該ネットワーク機器から前記アドレスの一覧表示を取得し、取得したアドレスのリストを検出部１２２に渡せばよい。

【００６４】

これにより、ネットワーク監視サーバ機１０５は、自分でネットワーク１０１を流れるパケットを傍受する必要がなくなり、図４に示すステップＳ４０１が不要となり、必要な処理能力を軽減することができる。

【００６５】

（応用例１）

本実施の形態のネットワーク監視サーバ機１０５を用いて、下記のようなサービス事業を実施することができる。すなわち、情報システム１００を保有する企業に対し、別のサービス事業者が、当該企業が保有するネットワーク監視サーバ機１０５の代わりに、当該サービス事業者の保有するネットワーク監視サーバ機を、前記企業の情報システム１００のネットワーク１０１に接続する。当該ネットワーク監視サーバ機は、監視ログ１２６の内容を、当該企業が改変できないように暗号化している他は、これまでに説明したネットワーク監視サーバ機１０５と同じである。前記サービス事業者は、前記企業から料金を取り、前記ネットワーク監視サーバ機の監視ログ１２６の内容を、当該企業及び当該サービス事業者とは異なる第三者に公証する。

【００６６】

このサービスにより、当該企業は、計量したオペレーショナルリスクが、当該企業内で業務に使うすべての計算機から損失イベントを抽出した結果であると、第三者により説得力のある形で示すことができる。また、当該サービス事業者は、前記の公証サービスを行うことによって、当該企業から収益を上げることがで

きる。

【００６７】

（応用例２）

本実施の形態の方法を用いて、下記のような保険業を実施することができる。すなわち、保険業者は、顧客企業から保険料を徴収し、もし当該企業に、オペレーショナルリスクに該当する原因により損失が発生した場合は、その損失に応じた保険金を支払う。ここで、保険業者は、当該顧客企業の情報システムにおいて、当該顧客企業の保有する業務実行計算機１０３ａ，１０３ｂ，…においてエージェント１１０を実行し、さらに運用管理サーバ機１０４とネットワーク監視サーバ機１０５をネットワーク１０１に接続する。

【００６８】

これにより、当該保険業者は、顧客企業のオペレーショナルリスクを正確に計量できる。そのため、リスクの大きさに応じて保険料を増減するなどのきめ細かな対応が可能となり、オペレーショナルリスクの小さい顧客企業に、より安い保険料を提示することにより保険の魅力を高めたり、リスクの大きい企業から安すぎる保険料しか取っていなかったために、保険金支払いにより損失を被ってしまう危険を低減したりできるようになる。

【００６９】

以上、本発明者によってなされた発明をその実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【００７０】

【発明の効果】

本願において開示される発明のうち、代表的なものによって得られる効果を簡単に説明すれば、以下のとおりである。

【００７１】

（１）業務実行計算機のエージェントによって収集された損失イベントから、オペレーショナルリスクを計算できるだけでなく、ネットワーク監視サーバ機の記録を検査することにより、企業内で業務に用いられる計算機すべてにおいて損

失イベントを収集したか否かを確認することができる。

【００７２】

（２）顧客企業内で業務に用いられる計算機のすべてから、損失イベントを収集したことを、第三者に対して保証するサービス事業を行い、収益を上げることができる。

【００７３】

（３）保険業者等が前記オペレーショナルリスク計量方法を顧客企業の情報システムに適用することにより、前記顧客企業のオペレーショナルリスクに該当する事象により発生した損失を正確に計量することが可能となり、当該損失を補填したり、当該計量結果に基づいて保険料を決定したりする保険業を運営することができる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態における情報システムのハードウェア及びソフトウェアの構成を示す図である。

【図２】

本発明の一実施の形態における、パケットの構造と内容を示す図である。

【図３】

本発明の一実施の形態における、運用管理サーバ機において実行する、オペレーショナルリスクの計量方法を示す流れ図である。

【図４】

本発明の一実施の形態において、ネットワーク監視サーバ機の検出部の動作を示す流れ図である。

【図５】

本発明の一実施の形態の第１の変形例において、情報システムがルータと１つ以上のサブネットワークから構成されている場合の、ハードウェア及びソフトウェアの構成を示す図である。

【符号の説明】

１００，５００　情報システム

１０１　ネットワーク

１０２　リンク

１０３ａ，１０３ｂ，５０３Ａａ，５０３Ａｂ，５０３Ｂａ，５０３Ｂｂ，…
業務実行計算機

１０４　運用管理サーバ機

１０５，５０５Ａ，５０５Ｂ　ネットワーク監視サーバ機

１１０　エージェント

１１１　データ収集部

１１２　確認応答部

１１５ａ，１１５ｂ，…　履歴情報

１２１　パケット監視部

１２２　検出部

１２５　アドレスリスト

１２６　監視ログ

１３１　データ集計部

１３２　計量部

１３３　結果表示部

２００　パケット

２０１　送信先アドレス

２０２　送信元アドレス

２０３　データ

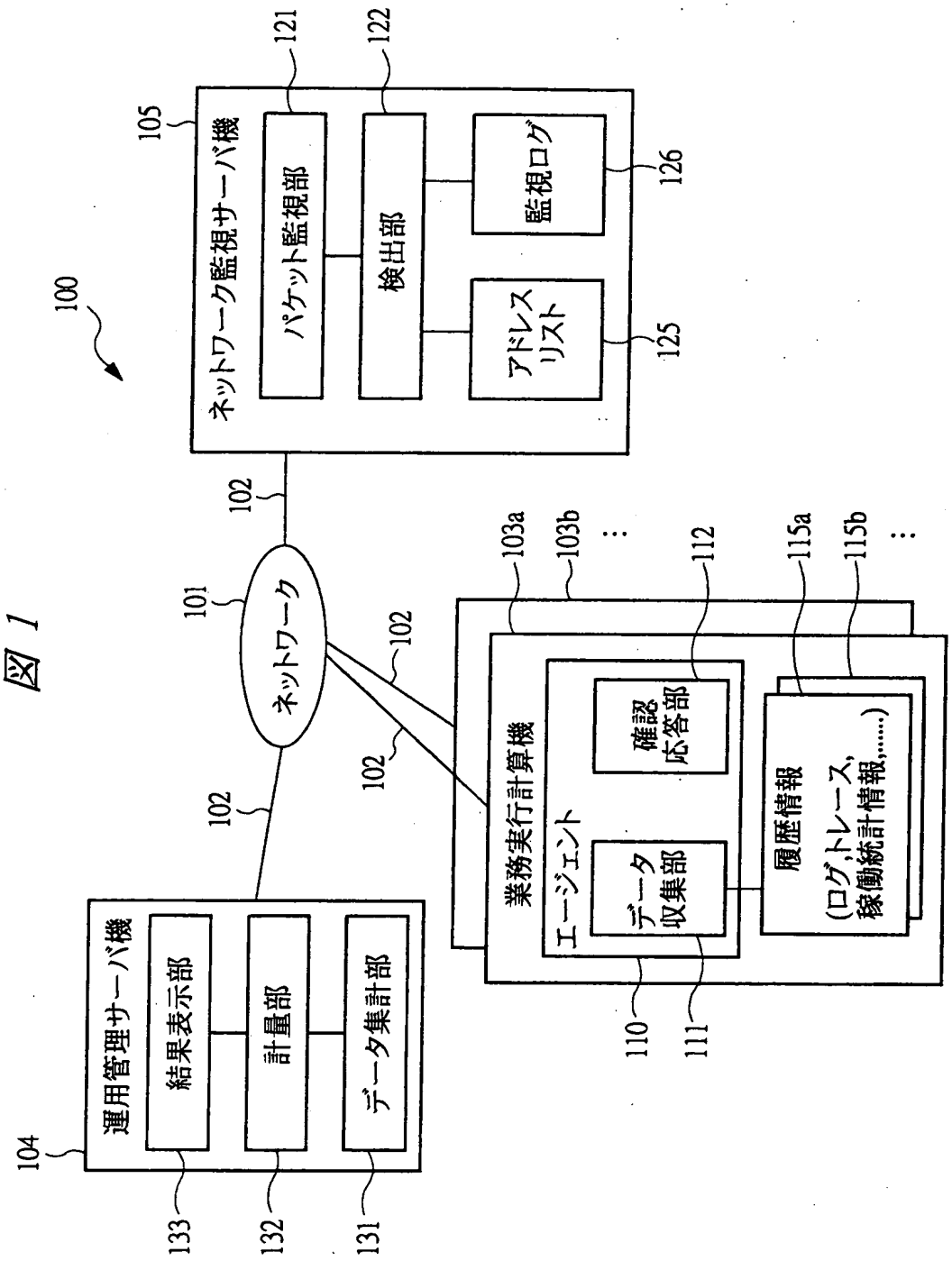
５０１Ａ，５０１Ｂ　サブネットワーク

５０２　ネットワーク機器（ルータ）

【書類名】　　図面

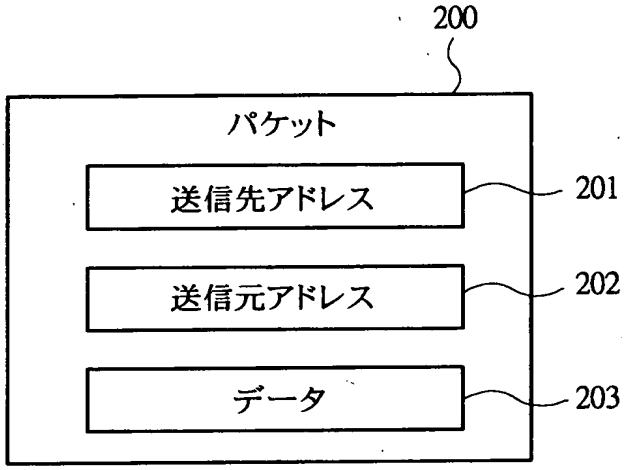
【図１】

図 1


100
101
102
103a
103b
104
105
110
111
112
115a
115b
121
122
125
126
131
132
133
ネットワーク
ネットワーク監視サーバ機
パケット監視部
検出部
監視ログ
アドレス
リスト
業務実行計算機
エージェント
データ
収集部
確認
応答部
履歴情報
(ログ,トレース,
稼働統計情報,.....)
運用管理サーバ機
結果表示部
計量部
データ集計部

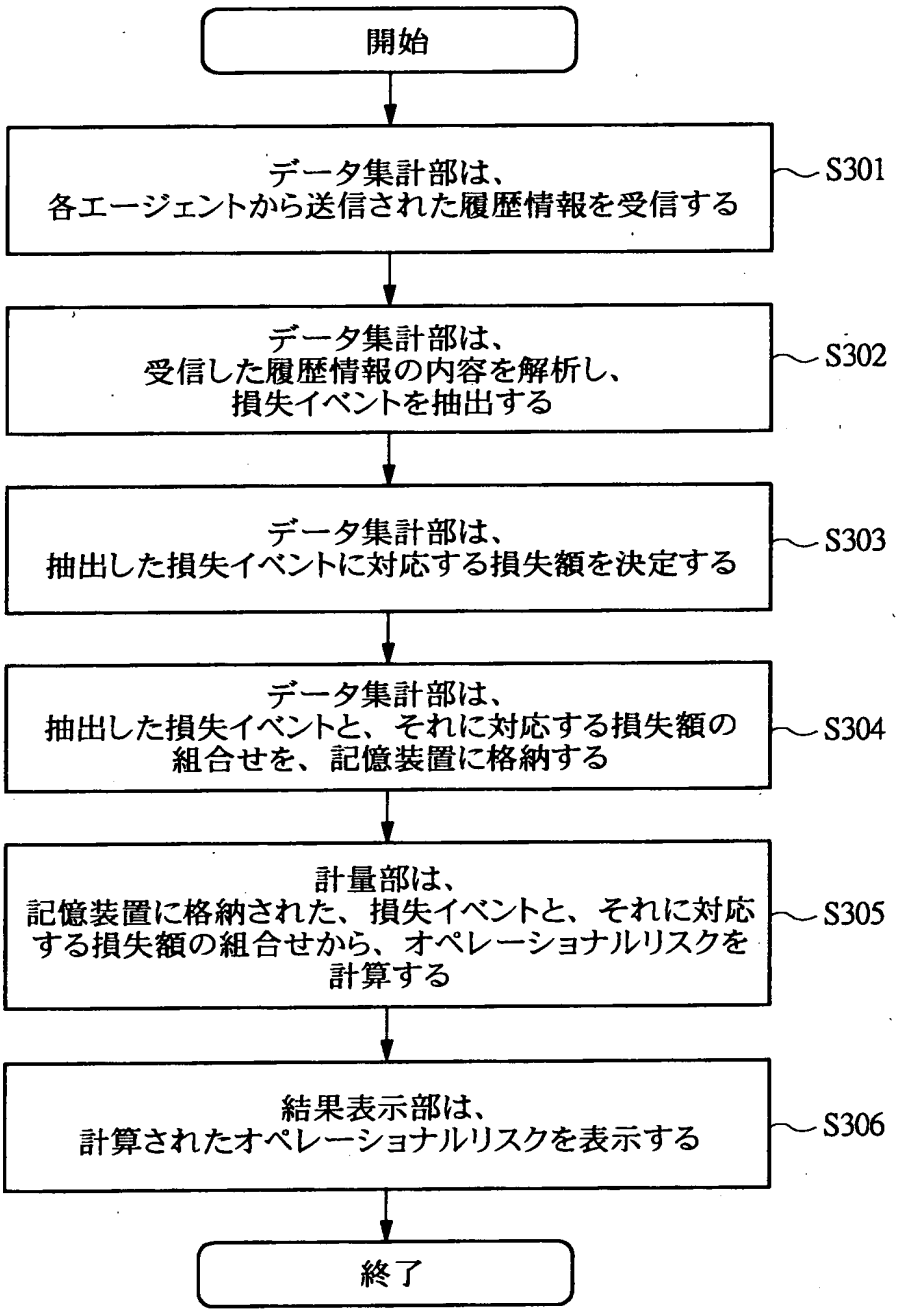
【図２】

図 2



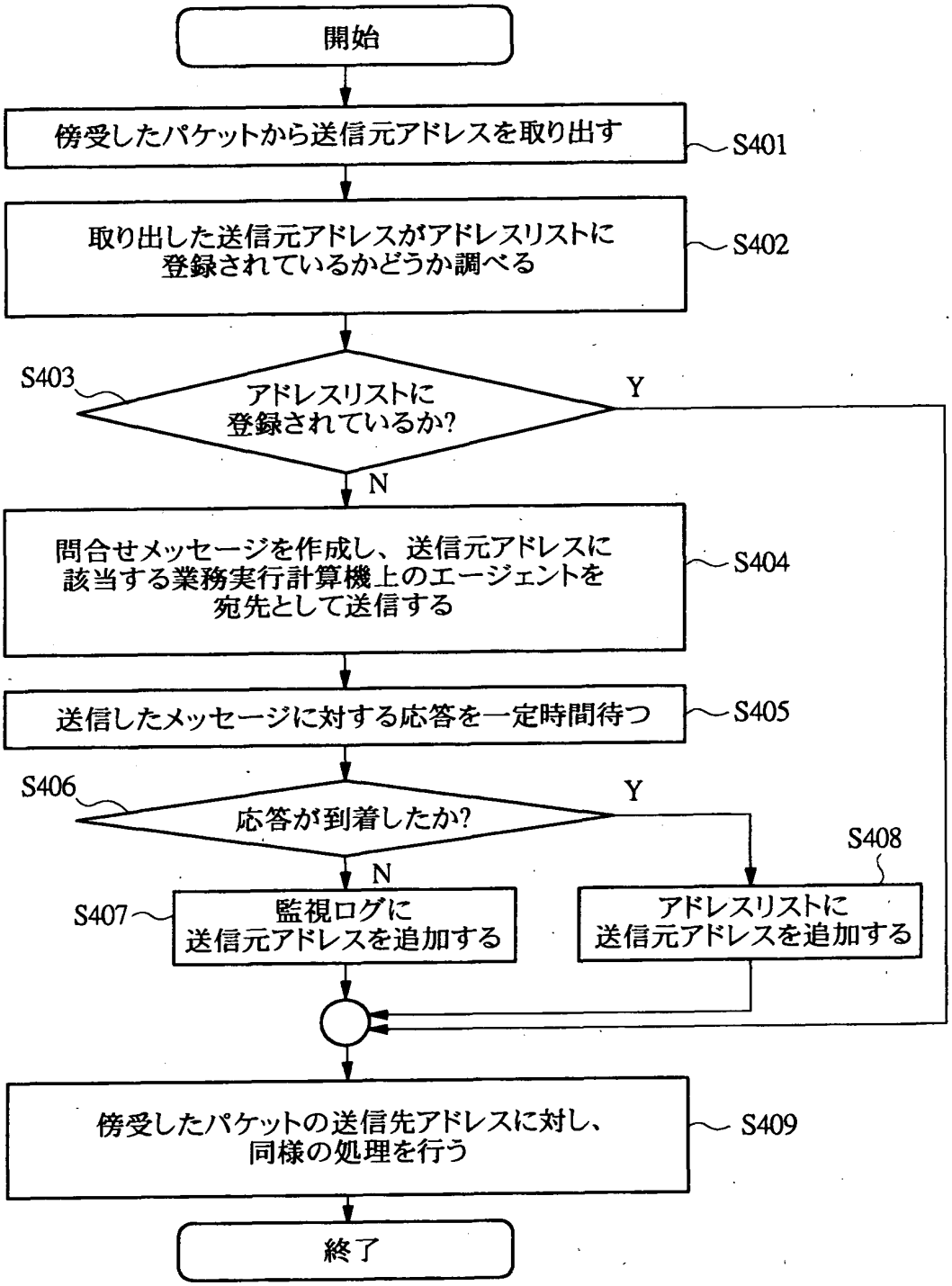
【図３】

図 3


開始
データ集計部は、
各エージェントから送信された履歴情報を受信する
S301
データ集計部は、
受信した履歴情報の内容を解析し、
損失イベントを抽出する
S302
データ集計部は、
抽出した損失イベントに対応する損失額を決定する
S303
データ集計部は、
抽出した損失イベントと、それに対応する損失額の
組合せを、記憶装置に格納する
S304
計量部は、
記憶装置に格納された、損失イベントと、それに対応
する損失額の組合せから、オペレーショナルリスクを
計算する
S305
結果表示部は、
計算されたオペレーショナルリスクを表示する
S306
終了

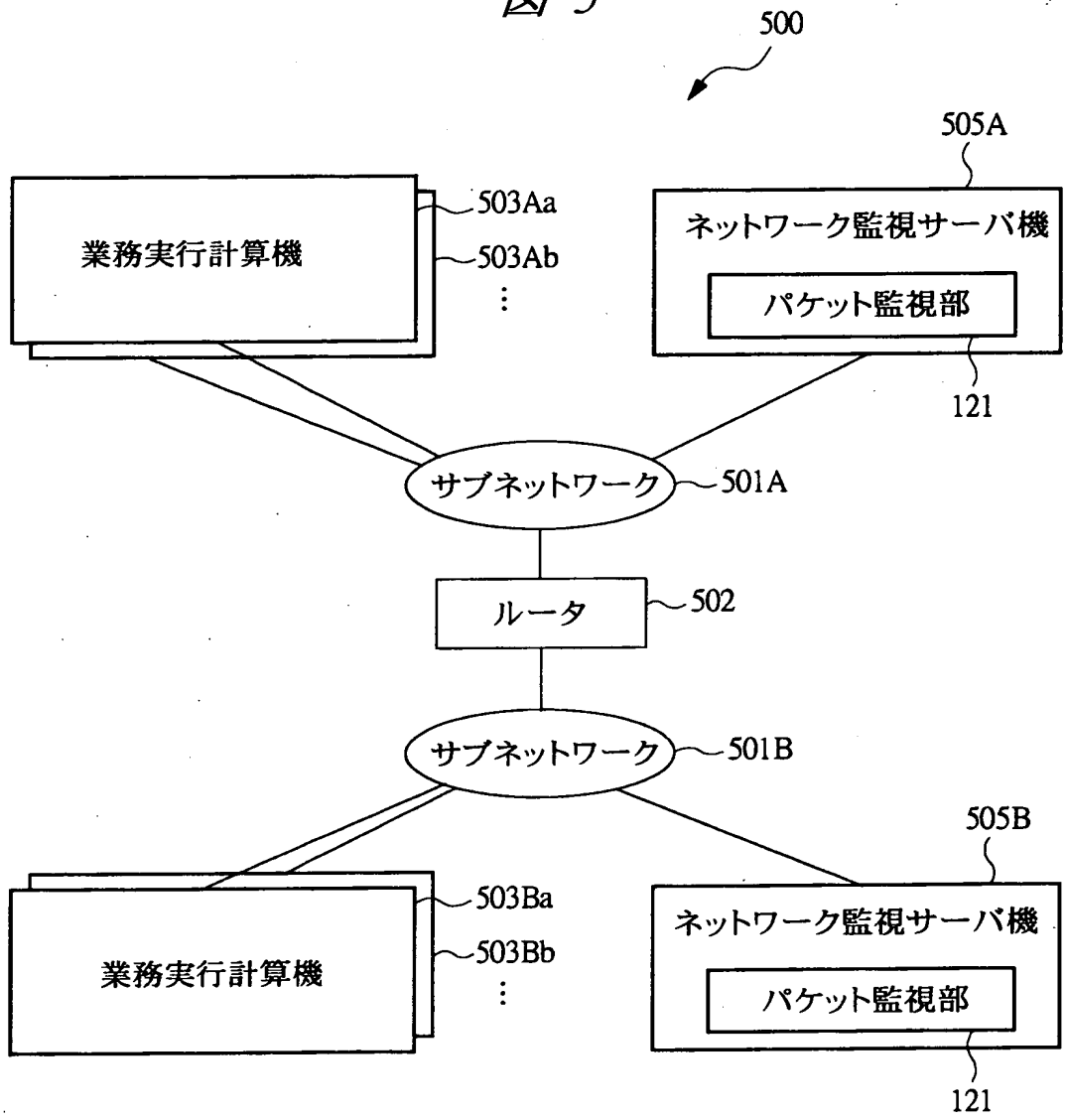
【図４】

図 4


開始
傍受したパケットから送信元アドレスを取り出す
S401
取り出した送信元アドレスがアドレスリストに登録されているかどうか調べる
S402
S403
アドレスリストに登録されているか?
Y
N
問合せメッセージを作成し、送信元アドレスに該当する業務実行計算機上のエージェントを宛先として送信する
S404
送信したメッセージに対する応答を一定時間待つ
S405
S406
応答が到着したか?
Y
N
S408
S407
監視ログに送信元アドレスを追加する
アドレスリストに送信元アドレスを追加する
傍受したパケットの送信先アドレスに対し、同様の処理を行う
S409
終了

【図５】

図 5


500
505A
503Aa
503Ab
業務実行計算機
ネットワーク監視サーバ機
パケット監視部
121
サブネットワーク
501A
ルータ
502
サブネットワーク
501B
505B
503Ba
503Bb
業務実行計算機
ネットワーク監視サーバ機
パケット監視部
121

【書類名】　　要約書

【要約】

【課題】　企業のオペレーショナルリスク計量のための内部データを、当該企業内のすべての計算機から収集したか否かを確認できる方法を提供する。

【解決手段】　業務実行計算機１０３ａ，１０３ｂ，…に、その計算機内で発生した損失イベントを収集するためのエージェント１１０を１つ以上設ける。また、その企業のネットワーク１０１に接続されたネットワーク監視サーバ機１０５を１つ以上設ける。ネットワーク監視サーバ機１０５は、ネットワーク１０１を監視し、業務実行計算機１０３ａ，１０３ｂ，…の中に、エージェント１１０が設けられていない計算機があれば、その旨を監視ログ１２６に追加することにより、企業内の業務を実行するすべての計算機について、内部データを収集するエージェント１１０が設けられているか否かを確認できるため、漏れのないオペレーショナルリスク計量が可能となる。

【選択図】　　図１

出証特２００３－３０３７８７６

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

1．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所